CNA e-Tool

Lender User and Coordinator

Access Guide

U.S. Department of Housing and Urban Development (HUD)

Federal Housing Administration (FHA)

June 2017

Document History

Version No.	Date	Author	Revision Description
1.0	08/17/2017	Sean Cortopassi	Final

Contents

1. Getting Started

The Capital Needs Assessment (CNA) e-Tool automates the process for the preparation, submission and review of a CNA. The CNA e-Tool home web page can be found at the following link: https://portal.hud.gov/hudportal/HUD?src=/program_offices/housing/mfh/cna

The CNA e-Tool is hosted on Secure Systems Platform. Lenders will request their Mortgagee ID from FHA Connection and it will be approved by their company coordinator. The Lender's company coordinator will grant the lender user their role(s). The coordinator should input the lender's account based on their home office as opposed to their branch office within FHA Connection when the account is being established. The Lenders will then login to FHA Connection which will take the user to Secure Systems where they can then access the CNA e-Tool to validate and then submit CNA's for HUD's review.

Obtaining access to any application is a two-step process consisting of authentication and authorization.

Lender User Authentication is a process of verifying user credentials on a system level to ensure that the user has access to the system in general. Lender User credentials are provided in the form of a username or user ID and a password, and are checked against an enterprise-level database called the Lightweight Directory Access Protocol (LDAP).

Lender User Authorization is done on an application level to determine what application and its function the user is authorized to access (in the case of lenders they can only be External Viewers and/or External Submitters). Authorization rights are typically set up by assigning application- specific roles and/or actions to the user ID inside the application database and are checked by the application process.

1.1 Intended Audience

This document is intended to serve as a user access guide for lenders and their company coordinator.

The following ID credential is available to the lender and the company coordinator:

- **Lender:** Mortgagee ID (M ID)
- **Lender Coordinator:** Mortgagee ID (M ID)

2. Lenders

Become an FHA-approved Lender

New lender applicants must complete an online application and attach the required documents in accordance with the FHA Housing Policy Handbook (Handbook 4000.1). In addition to submitting the required documentation, all lenders must confirm compliance through the Initial Certification Statements. Applicants must provide an explanation and supporting documentation for all negative responses.

Please do not create credentials until all documents are available to apply for FHA-approval. Once the account is created, the credentials will automatically expire after 120 days.

There are four types of FHA lender approvals:

Nonsupervised Mortgagee: Lending institutions may apply for this type of approval if they want to: originate, underwrite, close, endorse, service, purchase, hold, or sell FHA-insured Mortgages.

Supervised Mortgagee: Banks, savings banks and credit unions may apply for this type of approval if they want to: originate, underwrite, close, endorse, service, purchase, hold, or sell FHA-insured Mortgages.

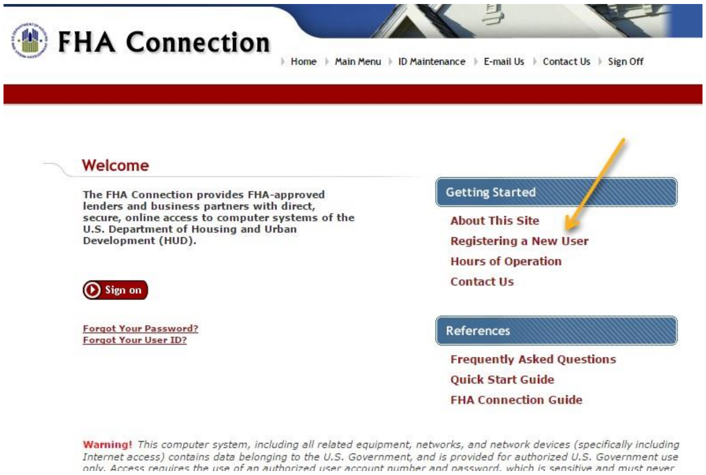
Government Mortgagee: Federal, state, or municipal government agencies, Federal Home Loan Banks, Freddie Mac or Fannie Mae may apply for this type of approval if they want to: originate, underwrite, close, endorse, service, purchase, hold, or sell FHA-insured Mortgages.

Investing Mortgagee: Organizations that want to invest funds under its own control may apply for this approval if they want to: purchase, hold, or sell FHA-insured Mortgages. An Investing Mortgagee may not originate, underwrite, or close FHA-insured Mortgages in its own name or submit applications for FHA mortgage insurance.

Lenders with questions who are currently preparing or planning to apply for FHA approval in the near future may contact the FHA Resource Center at answers@hud.gov or (800) 225-5342.

2.1 Lender Authentication

The very first thing an FHA-approved Lender should do is get an FHA Connection-issued M ID. Lender Users will access the CNA e-Tool through FHA Connection (which is the portal for lenders). Lenders will have a company coordinator, and that person will grant/revoke access to the CNA e-Tool through FHA Connection. Lenders will login with their M ID and password in FHA Connection. Information on obtaining an M ID can be found under Registering a New User on the FHA Connection public site at https://entp.hud.gov/clas/index.cfm.



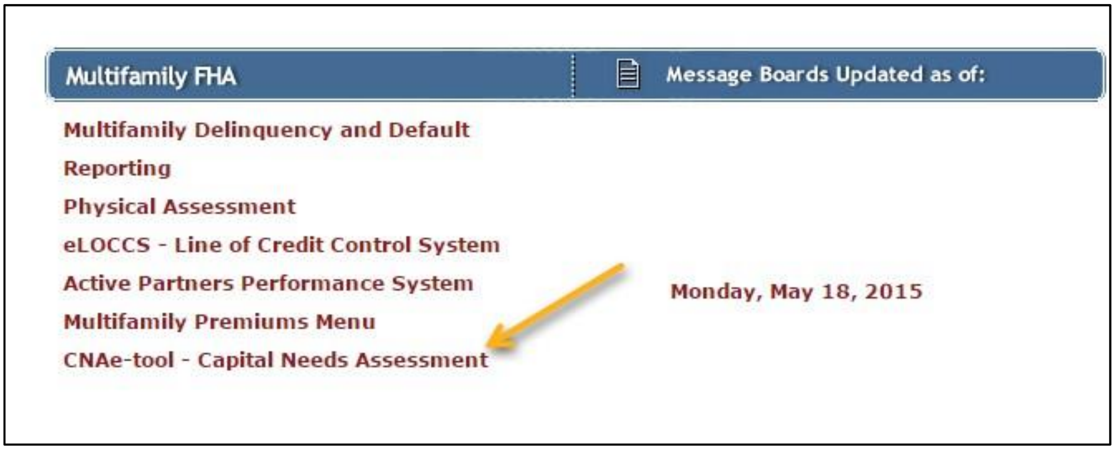
The FHA Connection provides FHA-approved lenders and business partners with direct, secure, online access to computer systems of the U.S. Department of Housing and Urban Development (HUD).

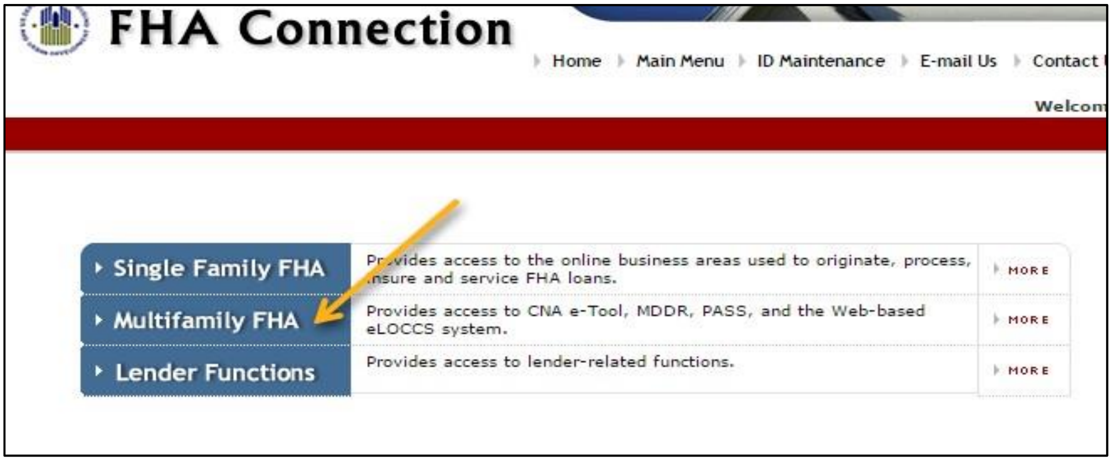
Warning! *This computer system, including all related equipment, networks, and network devices (specifically including Internet access) contains data belonging to the U.S. Government, and is provided for authorized U.S. Government use only. Access requires the use of an authorized user account number and password, which is sensitive and must never*

If the lender is running into issues with the FHA Connection registration process, then it is recommended that they read the link to this PDF which explains the registration procedure in elaborate detail: https://entp.hud.gov/pdf/mp_gs2_reguser.pdf and contact their company coordinator for assistance.

This link also discusses how a lender can register as a coordinator as well. The coordinator is responsible for assigning the External Viewer or Submitter role to the M ID lender users within their own company. Prior to receiving the M ID, the lender user may contact their coordinator to let them know that they need an M ID and whether they need a CNA e-Tool External Viewer or Submitter role within the CNA e-Tool. When FHA Connection issues the M ID, the system emails the user informing them that their M ID was issued. The coordinators are copied on this email so that the user has the email address of their coordinator to facilitate future communication if needed.

Once the lender user receives their M ID from their company's coordinator, they can access the CNA e-Tool screen by signing on at the FHA Connection screen and navigating to the Multifamily main menu. From the Multifamily FHA menu, the user will be redirected to the Secure Systems login screen and will be required to enter their credentials again. Single sign on between the FHA Connection and Secure Systems has not yet been implemented (therefore the user will need to sign on first to FHA Connection with their M ID and password, and again to Secure Systems with their M ID and password).


Multifamily FHA
Message Boards Updated as of:
Multifamily Delinquency and Default Reporting
Physical Assessment
eLOCCS - Line of Credit Control System
Active Partners Performance System
Multifamily Premiums Menu
CNAe-tool - Capital Needs Assessment
Monday, May 18, 2015

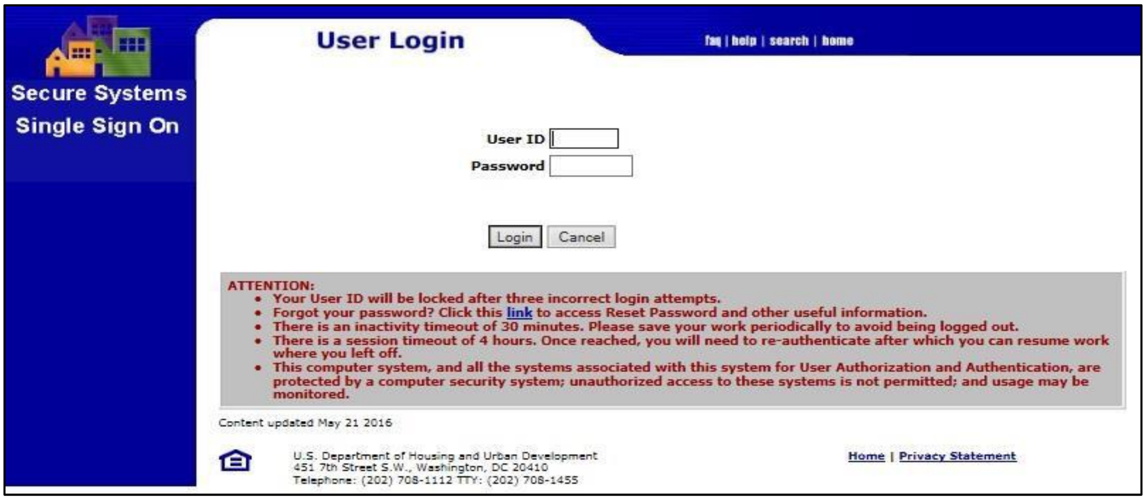


Provides access to the online business areas used to originate, process, insure and service FHA loans.

Provides access to CNA e-Tool, MDDR, PASS, and the Web-based eLOCCS system.

Provides access to lender-related functions.

What the Secure Systems Sign Screen will look like:



ATTENTION:

- Your User ID will be locked after three incorrect login attempts.
- Forgot your password? Click this link to access Reset Password and other useful information.
- There is an inactivity timeout of 30 minutes. Please save your work periodically to avoid being logged out.
- There is a session timeout of 4 hours. Once reached, you will need to re-authenticate after which you can resume work where you left off.
- This computer system, and all the systems associated with this system for User Authorization and Authentication, are protected by a computer security system; unauthorized access to these systems is not permitted; and usage may be monitored.

Content updated May 21 2016

U.S. Department of Housing and Urban Development
451 7th Street S.W., Washington, DC 20410
Telephone: (202) 708-1112 TTY: (202) 708-1455

Note: M ID users should remember to login to both FHA Connection and Secure Systems at least once every 90 days to ensure that their M ID is not locked due to inactivity. M ID Holders can access the CNA e-Tool application with their M ID through the Secure Systems website at the following link: https://hudapps.hud.gov/HUD_Systems

2.2 Lender Authorization

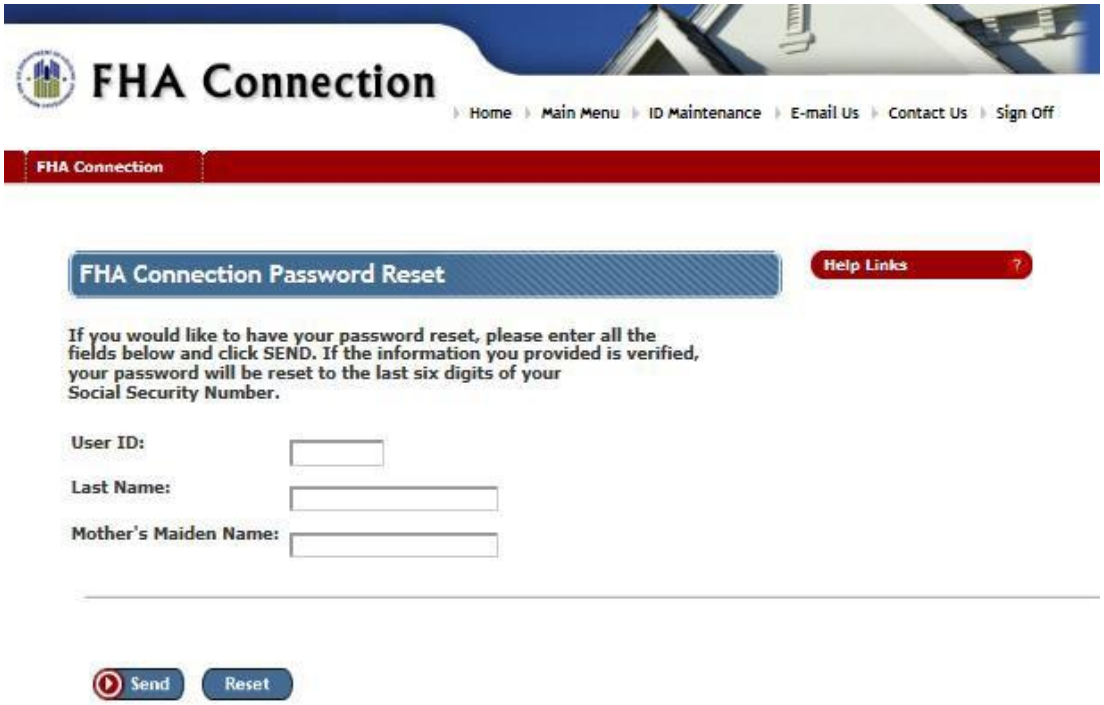
Lender CNA e-Tool Submitter or Viewer Roles are assigned to the user by their company's Lender Coordinator. Please refer to the FHA Connection user registration instructions for details.

2.3 Lender Help Desk Support

FHA Connection Issues

M ID holders receive assistance through the FHA Connection help desk email sfadmin@hud.gov, or by phone at 1-800-CALL-FHA. Note: Terminated M ID's are reactivated by their company's Coordinator.

If the M ID user needs to reset their FHA Connection Password, then they should go to the following link: https://entp.hud.gov/clas/f17pwd_reset_input.cfm. If the lender user would like to have their password reset, they will need to provide their M ID, last name, and mother's maiden name and click the Send Button. The lender user's password will be reset to the last six digits of their SSN.



FHA Connection Password Reset

If you would like to have your password reset, please enter all the fields below and click SEND. If the information you provided is verified, your password will be reset to the last six digits of your Social Security Number.

User ID:

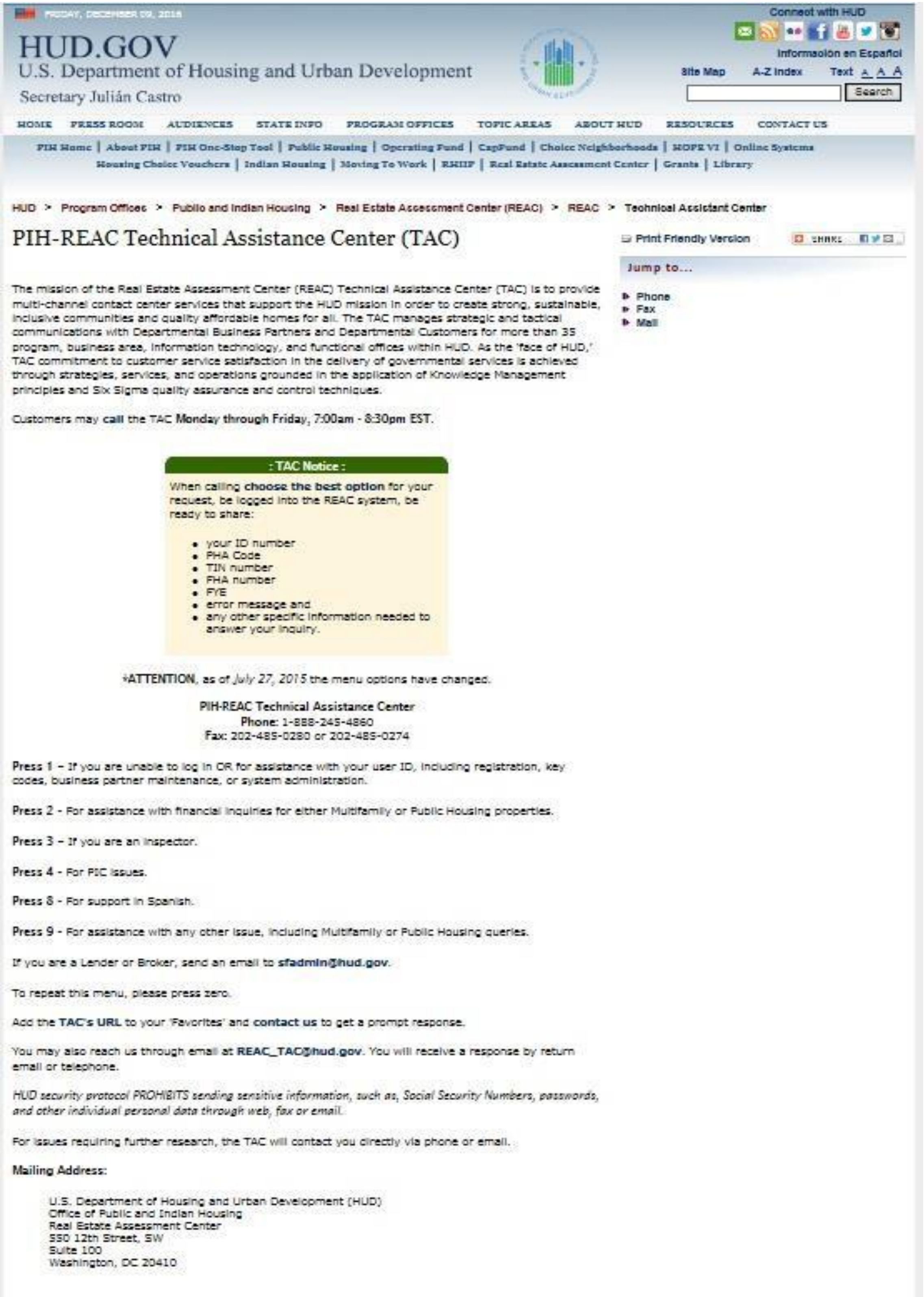
Last Name:

Mother's Maiden Name:

Note: M ID users should remember to login to FHA Connection at least once every 90 days to ensure that their M ID is not locked due to inactivity within FHA Connection.

Secure Systems Issues

Note that lender users get to the CNA e-Tool by accessing the Secure Systems Platform. Help desk support for M ID lender users who have issues with Secure Systems are provided by The Public and Indian Housing (PIH), The Real Estate Assessment Center (REAC), and The Technical Assistance Center (TAC). The help desk can be reached by phone at 1-888-245-4860 and is open Monday through Friday, 7:00am - 8:30pm EST. M ID lender users must change their Secure Systems Passwords frequently. M ID lender users will become inactive (requiring reactivation) after 90 days without logging into Secure System. In addition, PIH-REAC-TAC can be reached at the public website located at: http://portal.hud.gov/hudportal/HUD?src=/program_offices/public_indian_housing/reac/support/tac



FRIDAY, DECEMBER 09, 2016
Connect with HUD
Informacion en Español
Site Map
A-Z Index
Text A A A
Search
HOME
PRESS ROOM
AUDIENCES
STATE INFO
PROGRAM OFFICES
TOPIC AREAS
ABOUT HUD
RESOURCES
CONTACT US
PIH Home | About PIH | PIH One-Stop Tool | Public Housing | Operating Fund | CapFund | Choice Neighborhoods | HOPE VI | Online Systems
Housing Choice Vouchers | Indian Housing | Moving To Work | RHIIP | Real Estate Assessment Center | Grants | Library
HUD > Program Offices > Public and Indian Housing > Real Estate Assessment Center (REAC) > REAC > Technical Assistant Center
Print Friendly Version
SHARE
Jump to...
Phone
Fax
Mail

HUD.GOV
U.S. Department of Housing and Urban Development
Secretary Julián Castro

PIH-REAC Technical Assistance Center (TAC)

The mission of the Real Estate Assessment Center (REAC) Technical Assistance Center (TAC) is to provide multi-channel contact center services that support the HUD mission in order to create strong, sustainable, inclusive communities and quality affordable homes for all. The TAC manages strategic and tactical communications with Departmental Business Partners and Departmental Customers for more than 35 program, business area, information technology, and functional offices within HUD. As the 'face of HUD,' TAC commitment to customer service satisfaction in the delivery of governmental services is achieved through strategies, services, and operations grounded in the application of Knowledge Management principles and Six Sigma quality assurance and control techniques.

Customers may **call** the TAC **Monday through Friday, 7:00am - 8:30pm EST.**

: TAC Notice :

When calling **choose the best option** for your request, be logged into the REAC system, be ready to share:

- your ID number
- PHA Code
- TIN number
- FHA number
- FYE
- error message and
- any other specific information needed to answer your inquiry.

***ATTENTION**, as of *July 27, 2015* the menu options have changed.

PIH-REAC Technical Assistance Center
Phone: 1-888-245-4860
Fax: 202-485-0280 or 202-485-0274

Press 1 – If you are unable to log in OR for assistance with your user ID, including registration, key codes, business partner maintenance, or system administration.

Press 2 - For assistance with financial inquiries for either Multifamily or Public Housing properties.

Press 3 – If you are an inspector.

Press 4 - For PIC issues.

Press 8 - For support in Spanish.

Press 9 - For assistance with any other issue, including Multifamily or Public Housing queries.

If you are a Lender or Broker, send an email to **sfadmin@hud.gov**.

To repeat this menu, please press zero.

Add the **TAC's URL** to your 'Favorites' and **contact us** to get a prompt response.

You may also reach us through email at **REAC_TAC@hud.gov**. You will receive a response by return email or telephone.

HUD security protocol PROHIBITS sending sensitive information, such as, Social Security Numbers, passwords, and other individual personal data through web, fax or email.

For issues requiring further research, the TAC will contact you directly via phone or email.

Mailing Address:

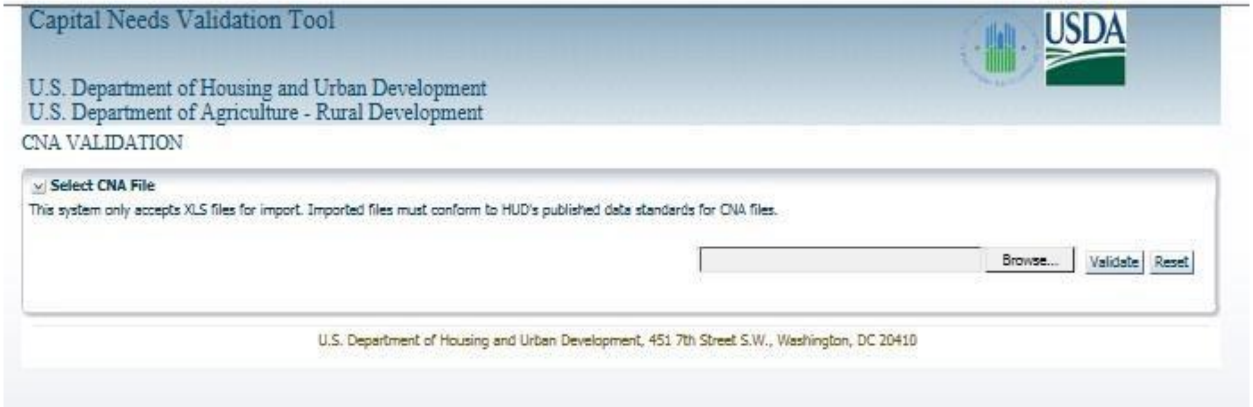
U.S. Department of Housing and Urban Development (HUD)
Office of Public and Indian Housing
Real Estate Assessment Center
550 12th Street, SW
Suite 100
Washington, DC 20410

3. CNA Validation Pages

The CNA Assessment Tool can be found on the CNA e-Tool web page at the following link: https://portal.hud.gov/hudportal/HUD?src=/program_offices/housing/mfh/cna

Public Validation Engine

Anyone who wish to validate CNA assessment data can access the public validation website without credentials directly at the following link: http://webapps.hud.gov/CNAeTool/faces/CnaValidation. Note: Needs Assessors are unlikely to need any kind of ID and will use the Public Validation Engine.



Capital Needs Validation Tool

U.S. Department of Housing and Urban Development
U.S. Department of Agriculture - Rural Development

CNA VALIDATION

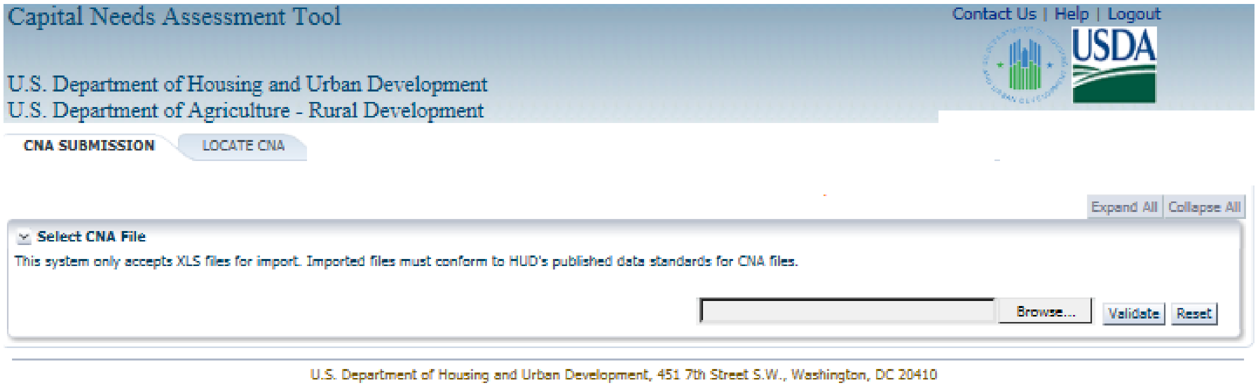
Select CNA File

This system only accepts XLS files for import. Imported files must conform to HUD's published data standards for CNA files.

U.S. Department of Housing and Urban Development, 451 7th Street S.W., Washington, DC 20410

Secure Validation Engine

When lender users are ready to submit their CNA for HUD's review, it must be validated in the Secure Validation Engine (which is located within the Submission Portal). Note that the lender user will need to login with their M ID and password. The Secure Validation Engine can be found at the following link: https://hudapps.hud.gov/HUD_Systems. And the Lender User will need to click the CNA Submission Tab.



Capital Needs Assessment Tool

U.S. Department of Housing and Urban Development
U.S. Department of Agriculture - Rural Development

Select CNA File

This system only accepts XLS files for import. Imported files must conform to HUD's published data standards for CNA files.

U.S. Department of Housing and Urban Development, 451 7th Street S.W., Washington, DC 20410

3.1 Help Desk Support for CNA Validation

If the lender user is having validation problems or questions with the assessment tool please send an email to CNAeTool@Hud.gov and attach screen shots of the error messages or issues observed. In addition, provide an explanation of the circumstances. Also, the lender user should provide their phone number, email, and any other contact information that they would like to provide to HUD.

4. Note about Personally Identifiable Information

During the registration and password reset processes the user may be required to provide their Social Security Number (SSN) and their mother's maiden name to complete the registration or password reset processes. The user may have concerns about providing that information on the Internet and are wondering why the forms require this sensitive personally identifiable information (PII).

According to government regulations, the SSN is required when trying to access a Federal computer system. HUD requires SSN and mother's maiden name to verify the users identity before processing the registration or password reset forms to issue an ID or reset your password. The information is being entered into a secure environment and will be used exclusively for the registration or password reset processes.

The user’s SSN and mother’s Maiden Name is considered PII. PII is protected by the Privacy Act of 1974, as amended (5 U.S. Code 552a). This information will only be used by Federal staff who hold positions of trust and who are specifically authorized to process ID credentials or reset passwords.

5. Note about sharing passwords and credentials

Users should never share their password or credential information with anyone (even if it is within their own company). This would be a violation of government regulations, and it increases the number of threats to HUD, Secure Systems, FHA Connection, and could potentially jeopardize PII. If it is determined that misuse with access ID has occurred there will be penalties and future access/credentials will be revoked. More information is provided within the Rules of Behavior, which we ask that the lender user please signs and email it to their company coordinator when the lender is applying for their M ID and CNA e-Tool Role (External Viewer and/or External Submitter).

Appendix A: CNA E-TOOL RULES OF BEHAVIOR

CNA E-TOOL RULES OF BEHAVIOR

SECTION I - RESPONSIBILITIES

This section describes what ROB are, why they are needed, what users can expect, and the consequences for violating the ROB.

What are Rules of Behavior?

Office of Management and Budget (OMB) Circular A-130 Appendix III requires every System Security Plan (SSP) to contain a Rules of Behavior (ROB). ROB apply to the system users and list specific responsibilities and expected behavior of all individuals with access to or use of the named information system. In addition, ROB outlines the consequences of non-compliance and/or violations.

Why are Rules of Behavior Needed?

ROB is part of a complete program to provide good information security and raise security awareness. ROB describes standard practices needed to ensure safe, secure, and reliable use of information and information systems.

Who is Covered by the Rules of Behavior?

The ROB covers all government and non-government users of the named information systems. This includes contract personnel and other federally funded users.

What are the Consequences for Violating the Rules of Behavior?

Penalties for non-compliance may include, but are not limited to, a verbal or written warning, removal of system access, reassignment to other duties, demotion, suspension, reassignment, termination, and possible criminal and/or civil prosecution.

SECTION II - APPLICATION AND ORGANIZATION RULES

This section identifies the Rules of Behavior measures that will apply to Capital Needs Assessment Electronic Tool end-users. Section 3.1 lists the most common and minimal set of ROB as recommended by NIST 800-18. Section 3.2 lists other ROB that may apply to your organization. Section 2h includes ROB for system administrators. Each section is discussed in detail below.

A. Passwords

1. Passwords should be a minimum of eight characters, and be a combination of letters, numbers and special characters (such as *#$ %). Dictionary words should not be used.
2. Passwords will be changed at least every 90 days and should never be repeated. Compromised passwords will be changed immediately.
3. Passwords must be unique to each user and must never be shared by that user with other users. For example, colleagues sharing office space must never share each other's password to gain system access.
4. Users who require multiple passwords should never be allowed to use the same password for multiple applications.
5. Passwords must never be stored in an unsecured location. Preferably, passwords should be memorized. If this is not possible, passwords should be kept in an approved storage device, such as a Government Services Administration Security Container. If they are stored on a computer, this computer should not be connected to a network or the Internet. The file should be encrypted.

B. Encryption

1. Extremely sensitive data should be encrypted prior to transmission.
2. The sensitivity of the information needing protection, among other considerations, determines the sophistication of the encryption technology. In most circumstances, only the most sensitive or compartmentalized information should be encrypted.
3. Files that contain passwords, proprietary, personnel, or business information, and financial data typically require encryption before transmission, and should be encrypted while stored on the computer's hard disk drive.
4. Sensitive information that travels over wireless networks and devices should be encrypted.

C. Internet Usage

1. Downloading files, programs, templates, images, and messages, except those explicitly authorized and approved by the system administrator, is prohibited.
2. Visiting websites including, but not limited to, those that promote, display, discuss, share, or distribute hateful, racist, pornographic, explicit, or illegal activity is strictly prohibited.
3. Because they pose a potential security risk, the use of Web based instant messaging or communication software or devices are prohibited.
4. Using the Internet to make non-work related purchases or acquisitions is prohibited.
5. Using the Internet to manage, run, supervise, or conduct personal business enterprises is prohibited.

D. Email

1. Except for limited personal use, non-work-related e-mail is prohibited. The dissemination of e-mail chain letters, e-mail invitations, or e-mail cards is prohibited.
2. E-mail addresses and e-mail list-serves constitute sensitive information and are never to be sold, shared, disseminated, or used in any unofficial manner.
3. Using an official e-mail address to subscribe to any non-work related electronically distributed newsletter or magazine is prohibited.

E. Working from Home/Remote Dial-up Access

All CNA E-TOOL users are responsible for attending annual IT Security certification training. Failure to attend will result in having system access privileges revoked.

1. Users may dial into the network remotely only if pre-approved by the system administrator.
2. Users must be certain to log-off and secure all connections/ports upon completion.
3. Users who work from home must ensure a safe and secure working environment free from unauthorized visitors. At no time should a “live” dial-up connection be left unattended.
4. Web browsers must be configured to limit vulnerability to an intrusion and increase security.
5. Home users connected to the Internet via a broadband connection (e.g. DSL or a cable-modem) must install a hardware or software firewall.
6. No official material may be stored on the user’s personal computer. All data must be stored on a floppy disk and then secured in a locked filing cabinet, locker, etc.
7. Operating system configurations should be selected to increase security.

F. Unofficial Use of Government Equipment

Except for limited personal use, government equipment including, but not limited to, fax machines, copying machines, postage machines, telephones, and computers are for official use only.

G. Other Rules of Behavior

To properly safeguard the Department's information assets while using information technology, it is essential for all employees to be aware of procedures for destroying sensitive information. Sensitive information within HUD that must be protected includes, but is not limited to, financial management information (budgeting, accounting, etc.); investigative information; contract sensitive information (pre-solicitation procurement documents, statements of work, etc.); and security management information (i.e., identification of systems security controls and vulnerabilities).

Of particular concern is Personally Identifiable Information (PII), which includes social security numbers, names, dates of birth, places of birth, parents' names, credit card numbers, applications for entitlements, and information relating to a person's private financial, income, employment, tax records, etc.

To assist you in determining what type of information should be considered sensitive, here are a few examples:

1. Personnel data
2. Travel vouchers
3. Procurement documents
4. Statements of Work or related procurement documents
5. Loan applications or files
6. Grant applications or files
7. COOP data

The May 25, 2006 memorandum from the Deputy Secretary and the June 6, 2006 broadcast email from the CIO to all HUD employees stated "Protect all electronic/optical media and hard copy documentation containing sensitive information and properly dispose of it by shredding hard copy documentation, or by contacting the HITS Help Desk to dispose of electronic/optical media".

In each Regional Office a location will be set up, in the Information Technology Division, where media containing sensitive data will be destroyed.

Please use the following procedures to properly destroy sensitive data stored on electronic/optical media that are no longer in need of maintaining:

1. Contact your supporting IT staff if you need media destroyed that contains sensitive information (CDs, DVDs, flash drives, Personal Verification Cards (PVC), external hard drives, etc.) and you will be provided with instructions.

In addition, absolutely no media containing sensitive information will be sent through the mail or released from the Department.

1. Using system resources to copy, distribute, utilize, or install unauthorized copyrighted material is prohibited.
2. Users who no longer require IT system access (as a result of job change, job transfer, or reassignment of job responsibilities) must notify the system administrator.
3. When not in use, workstations must be physically secured. Users must also log-off or turn-off the system.
4. Screen-savers must be password protected.
5. Movable media (such as diskettes, CD-ROMs, and Zip disks) that contain sensitive and/or official information must be secured when not in use.
6. Altering code, introducing malicious content, denying service, port mapping, engaging a network sniffer, or tampering with another person’s account is prohibited.
7. If a user is locked out of the system, the user should not attempt to log-on as someone else. Rather, the user should contact the system administrator.

H. Additional Rules of Behavior for CNA e-TOOL System Administrators

CNA e-TOOL system administrators have a unique responsibility above and beyond that of regular users. In addition to being regular system users, they also have special access privileges that regular users do not have. Therefore, they need to be susceptible to additional Rules of Behavior over and above the common user.

1. CNA e-TOOL System administrators may only access or view user accounts with the expressed consent of the user and/or management.
2. CNA e-TOOL System administrators may not track or audit user accounts without the expressed consent of the user and/or management.
3. CNA e-TOOL System administrators must make every reasonable effort to keep the network free from viruses, worms, Trojans, and unauthorized penetrations.
4. It is the CNA e-TOOL system administrators’ responsibility to account for all system hardware and software loaned to system users for the execution of their official duties.
5. CNA e-TOOL system administrators are responsible for attending annual IT Security certification training. Failure to attend will result in having system access privileges revoked.

SECTION III - ACKNOWLEDGMENT

Prior to receiving authorization for CNA E-TOOL system access, every user should read and sign the ROB (this applies to system administrators since they are also "users" of the system). By signing the signature page, the user agrees to abide by the ROB and understands that failure to do so might be grounds for disciplinary action. Please retain a signed copy of the ROB for your personal records and submit the original signed copy to the CNA E-TOOL System Administrator for your local office.

I have read and understand the Rules of Behavior (ROB) governing my use of the Capital Needs Assessment Electronic Tool (CNA E-TOOL) and agree to abide by them. I understand that failure to do so may result in disciplinary action being brought against me.

NAME (PRINT)	ORGANIZATION
SIGNATURE	DATE SIGNED